МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Комплексные системы защиты информации на предприятии

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **4**
Семестр: **7, 8**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	8 семестр	Всего	Единицы
1	Лекции	36		36	часов
2	Практические занятия	66	8	74	часов
3	Лабораторные работы		24	24	часов
4	Контроль самостоятельной работы (курсовой проект / курсовая работа)		10	10	часов
5	Всего аудиторных занятий	102	42	144	часов
6	Из них в интерактивной форме	20	12	32	часов
7	Самостоятельная работа	78	66	144	часов
8	Всего (без экзамена)	180	108	288	часов
9	Подготовка и сдача экзамена	36		36	часов
10	Общая трудоемкость	216	108	324	часов
		6.0	3.0	9.0	З.Е

Экзамен: 7 семестр
Зачет: 8 семестр
Курсовая работа (проект): 8 семестр

Томск 2017

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент каф. РЗИ _____ А. П. Кшнянкин

Заведующий обеспечивающей каф. РЗИ _____ А. С. Задорин

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РЗИ _____ А. С. Задорин

Эксперты:

ведущий инженер каф. РЗИ РТФ _____ Ю. В. Зеленецкая

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является формирование у студентов устойчивых основ знаний организации комплексных систем защиты информации на предприятии и методов ее управления, приобретения при этом необходимых умений и навыков.

1.2. Задачи дисциплины

- Основными задачами изучения дисциплины являются:
- • изучение сущности и задач комплексной системы защиты информации (КСЗИ);
- • изучение принципов организации и этапов разработки КСЗИ, факторов, влияющих на организацию КСЗИ;
- • определение и нормативное закрепление состава защищаемой информации; определение объектов защиты;
- • анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию;
- • определение потенциальных каналов и методов несанкционированного доступа к информации, определение возможностей несанкционированного доступа к защищаемой информации;
- • определение компонентов и условий функционирования КСЗИ, разработка модели, технологического и организационного построения КСЗИ;
- • кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ;
- • назначение, структура и содержание управления КСЗИ, изучение принципов и методы планирования, сущности и содержание контроля функционирования КСЗИ;
- • изучение особенностей управления КСЗИ в условиях чрезвычайных ситуаций;
- • изучение состава методов и моделей оценки эффективности КСЗИ.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Комплексные системы защиты информации на предприятии» (Б1.В.ОД.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Защита и обработка конфиденциальных документов, Защита информационных процессов в компьютерных системах, Информационные технологии, Криптографические методы защиты информации, Оптимизация средств информационной безопасности, Организационное и правовое обеспечение информационной безопасности, Организация и управление службой защиты информации на предприятии, Основы информационной безопасности, Программно-аппаратные средства защиты информации, Системы видеонаблюдения, контроля доступа и охраны, Техническая защита информации, Управление информационной безопасностью, Экономика защиты информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
- ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

В результате изучения дисциплины студент должен:

- **знать** Основы организации и управления комплексной системой защиты информации на предприятии.
- **уметь** На концептуальном и практическом уровне разрабатывать и внедрять

комплексные системы защиты информации на предприятии.

– **владеть** Навыками внедрения комплексных систем защиты информации на предприятии.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 9.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		7 семестр	8 семестр
Аудиторные занятия (всего)	144	102	42
Лекции	36	36	
Практические занятия	74	66	8
Лабораторные работы	24		24
Контроль самостоятельной работы (курсовой проект / курсовая работа)	10		10
Из них в интерактивной форме	32	20	12
Самостоятельная работа (всего)	144	78	66
Оформление отчетов по лабораторным работам	30		30
Проработка лекционного материала	30	30	
Подготовка к практическим занятиям, семинарам	84	48	36
Всего (без экзамена)	288	180	108
Подготовка и сдача экзамена	36	36	
Общая трудоемкость ч	324	216	108
Зачетные Единицы	9.0	6.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические	Лабораторные	Самостоятельная работа	Контроль (без	Компетенции
7 семестр						
1 Введение.	1	6	0	8	0	15	ПК-10, ПК-13, ПК-4
2 Содержание и этапы проведения работ по организации комплексной системы защиты информации.	5	8	0	10	0	23	ПК-10, ПК-13
3 Определение компонентов КСЗИ.	9	8	0	10	0	27	ПК-10, ПК-13, ПК-4
4 Технология определения и классификации состава и защищенности информации.	7	16	0	9	0	32	ПК-10, ПК-13, ПК-4
5 Построение комплексной	4	18	0	24	0	46	ПК-10, ПК-

системы защиты информации.							13, ПК-4
6 Управление комплексной системой защиты информации.	2	10	0	8	0	20	ПК-10, ПК-4
7 Служба защиты информации.	4	0	0	3	0	7	ПК-10, ПК-13
8 Особенностей управления КСЗИ в условиях чрезвычайных ситуаций.	2	0	0	3	0	5	ПК-10, ПК-13, ПК-4
9 Состав методов и моделей оценки эффективности КСЗИ.	2	0	0	3	0	5	ПК-10, ПК-13, ПК-4
10 Экзамен.	0	0	0	0	0	0	
Итого за семестр	36	66	0	78	0	180	
8 семестр							
11 Зачёт.	0	8	24	66	10	98	ПК-10, ПК-13, ПК-4
Итого за семестр	0	8	24	66	10	108	
Итого	36	74	24	144	10	288	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Осваиваемые компетенции
7 семестр			
1 Введение.	Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению комплексной системы защиты информации на предприятии. Специфика курса.	1	ПК-10, ПК-13, ПК-4
	Итого	1	
2 Содержание и этапы проведения работ по организации комплексной системы защиты информации.	Цели комплексной защиты информации (ЗИ) и способы ее обеспечения. Системный метод при решении задач обеспечения комплексной защиты информации.Определение возможных каналов утечки информации. Определение объектов и элементов защиты.Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации. Выбор методов и средств защиты информации	5	ПК-10, ПК-13
	Итого	5	

3 Определение компонентов КСЗИ.	Правовая защита информации. Законодательная база по ЗИ. Сертификация и лицензирование. Правовые нормы, методы и средства защиты охраняемой информации в РФ. Система юридической ответственности за нарушение норм защиты государственной, служебной и коммерческой тайны в РФ. Правовые основы выявления и предупреждения утечки охраняемой информации.Техническая защита информации. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлектронный). Методы защиты от несанкционированного перехвата речевой, визуальной, оптической, радиоэлектронной информации. Радиомониторинг. Криптографическая защита информации. Средства и методы.Физическая защита информации. Принципы, силы, средства и условия организационной защиты информации. Организация внутриобъектового и пропускного режима предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа). Организация аналитической работы по предупреждению перехвата конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Определение политики защиты информации на предприятии. Особенности организации комплексной защиты информации, отнесенной в установленном порядке к государственной тайне. Определение сил и средств, необходимых для защиты информации.	9	ПК-10, ПК-13, ПК-4
	Итого	9	
4 Технология определения и классификации состава и защищенности информации.	Охраняемые сведения и объекты защиты.Особенности отнесения сведений, составляющих служебную, конфиденциальную, коммерческую и	7	ПК-13

	государственную тайну к различным степеням и категориям доступа.		
	Итого	7	
5 Построение комплексной системы защиты информации.	Разработка моделей комплексной системы защиты информации. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИАрхитектурное построение комплексной системы защиты информации.	4	ПК-10, ПК-13, ПК-4
	Итого	4	
6 Управление комплексной системой защиты информации.	Структура и содержание технологии управления комплексной системой защиты информации. Планирование и оперативное управление системой ЗИ, управление КСЗИ в условиях чрезвычайных ситуаций.Анализ надежности функционирования комплексной системы защиты информации.	2	ПК-10, ПК-4
	Итого	2	
7 Служба защиты информации.	Организация службы защиты информации (СЗИ) и организационное проектирование деятельности СЗИ. Порядок создания СЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации.	4	ПК-10, ПК-13
	Итого	4	
8 Особенностей управления КСЗИ в условиях чрезвычайных ситуаций.	Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и обеспечение КСЗИ. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИПонимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер	2	ПК-10, ПК-13, ПК-4

	КСЗИ.Восстановление после чрезвычайной ситуации функций и механизмов КСЗИ организации. Организационная основа процессов восстановления, вопросы системы менеджмента информационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации		
	Итого	2	
9 Состав методов и моделей оценки эффективности КСЗИ.	Основные термины и определения, характеризующие эффективность защиты информации. Содержание и особенности методологии оценки эффективности КСЗИ.Основные модели оценки эффективности КСЗИ.	2	ПК-10, ПК-13, ПК-4
	Итого	2	
Итого за семестр		36	
Итого		36	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин										
	1	2	3	4	5	6	7	8	9	10	11
Предшествующие дисциплины											
1 Защита и обработка конфиденциальных документов		+			+	+					
2 Защита информационных процессов в компьютерных системах			+	+	+						
3 Информационные технологии		+	+	+	+						
4 Криптографические методы защиты информации			+								
5 Оптимизация средств информационной безопасности				+	+						
6 Организационное и правовое обеспечение информационной		+				+	+				

безопасности											
7 Организация и управление службой защиты информации на предприятии						+	+	+			
8 Основы информационной безопасности			+								
9 Программно-аппаратные средства защиты информации			+								
10 Системы видеонаблюдения, контроля доступа и охраны					+						
11 Техническая защита информации		+	+	+	+				+		
12 Управление информационной безопасностью						+	+	+	+		
13 Экономика защиты информации									+		

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий					Формы контроля
	Лекции	Лабораторные работы	Практические занятия	Работы (курсовое проектирование)	Самостоятельная работа	
ПК-4	+	+	+	+	+	Экзамен, Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов (работ), Зачет, Выступление (доклад) на занятии, Отчет по курсовой работе
ПК-10	+	+		+	+	Экзамен, Конспект самоподготовки, Опрос на занятиях, Защита курсовых проектов (работ), Зачет, Выступление (доклад) на занятии, Отчет по курсовой работе

ПК-13	+	+		+	+	Экзамен, Конспект самоподготовки, Опрос на занятиях, Защита курсовых проектов (работ), Зачет, Выступление (доклад) на занятии, Отчет по курсовой работе

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Интерактивные лабораторные занятия	Всего
7 семестр				
Мозговой штурм	6	4		10
Решение ситуационных задач	4	2		6
Презентации с использованием слайдов с обсуждением	2	2		4
Итого за семестр:	12	8	0	20
8 семестр				
Мозговой штурм	2		2	4
Разработка проекта	4		4	8
Итого за семестр:	6	0	6	12
Итого	18	8	6	32

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	[illegible]	[illegible]
8 семестр			
11 Зачёт.	Система защиты информации от несанкционированного доступа SecretNet.	4	ПК-4
	Система защиты информации от несанкционированного доступа Dallas Lock.	4	
	Система защиты информации от несанкционированного доступа Страж NT.	4	
	DLP-решения по защите информации в информационных системах.	4	
	Защита информации от программных	4	

	воздействий на базе антивируса Dr.Web.		
	Защита информации от программных воздействий на базе антивируса KAV.	4	
	Итого	24	
Итого за семестр		24	
Итого		24	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Введение.	Сущность и понятие системы защиты информации с позиции системного подхода.	6	ПК-10, ПК-13, ПК-4
	Итого	6	
2 Содержание и этапы проведения работ по организации комплексной системы защиты информации.	Сущность и понятие объекта защиты информации, объекта информатизации.	8	ПК-10, ПК-13
	Итого	8	
3 Определение компонентов КСЗИ.	Определение, понятие и физический смысл технического канала утечки информации (ТКУИ). Методология защиты информации от утечки по техническим каналам.	8	ПК-10, ПК-13, ПК-4
	Итого	8	
4 Технология определения и классификации состава и защищенности информации.	Помещения, предназначенные для конфиденциальных переговоров. ТКУИ, характерные для объекта защиты. Определения и понятия. Методика защиты информации.Обработка защищаемой информации с использованием технических средств и систем. ТКУИ, характерные для объекта защиты. Определения и понятия.Методика защиты информации.	16	ПК-10, ПК-13, ПК-4
	Итого	16	
5 Построение комплексной системы защиты информации.	Защита информации от несанкционированного доступа (НСД). Основные определения и понятия. Особенности защиты от НСД к информации в автоматизированных системах и средствах вычислительной техники.Модель угроз и нарушителя. Понятие и основные практические	18	ПК-10, ПК-13, ПК-4

	подходы к разработке.Средства защиты информации по ТКУИ. Особенности выбора и обоснования.		
	Итого	18	
6 Управление комплексной системой защиты информации.	Аттестация объектов информатизации по требованиям безопасности информации.Основнае понятия и особенности практической реализации. Состав примерного комплекта документов.	10	ПК-10, ПК-4
	Итого	10	
Итого за семестр		66	
8 семестр			
11 Зачёт.	Договор на проведение аттестации объекта информатизации по требованиям безопасности информации. Сущность, состав и особенности.	2	ПК-10, ПК-13, ПК-4
	Техническое задание на проведение аттестации объекта информатизации по требованиям безопасности информации. Сущность, состав и особенности.	2	
	Технический паспорт защищаемого объекта информатизации. Сущность, состав и особенности.Особенности подготовки технического паспорта объекта вычислительной техники (ОВТ).	2	
	Особенности разработки системы защиты информации персональных данных в информационных системах.	2	
	Итого	8	
Итого за семестр		8	
Итого		74	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость,	Формируемые компетенции	Формы контроля
7 семестр				
1 Введение.	Подготовка к практическим занятиям, семинарам	6	ПК-10, ПК-13, ПК-4	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	2		

	Итого	8		
2 Содержание и этапы проведения работ по организации комплексной системы защиты информации.	Подготовка к практическим занятиям, семинарам	6	ПК-10, ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	4		
	Итого	10		
3 Определение компонентов КСЗИ.	Подготовка к практическим занятиям, семинарам	6	ПК-10, ПК-13, ПК-4	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	4		
	Итого	10		
4 Технология определения и классификации состава и защищенности информации.	Подготовка к практическим занятиям, семинарам	6	ПК-10, ПК-13, ПК-4	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	3		
	Итого	9		
5 Построение комплексной системы защиты информации.	Подготовка к практическим занятиям, семинарам	18	ПК-10, ПК-13, ПК-4	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	6		
	Итого	24		
6 Управление комплексной системой защиты информации.	Подготовка к практическим занятиям, семинарам	6	ПК-10, ПК-4	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен
	Проработка лекционного материала	2		
	Итого	8		
7 Служба защиты информации.	Проработка лекционного материала	3	ПК-10, ПК-13	Конспект самоподготовки, Опрос на занятиях, Экзамен
	Итого	3		
8 Особенностей управления КСЗИ в условиях чрезвычайных ситуаций.	Проработка лекционного материала	3	ПК-10, ПК-13, ПК-4	Конспект самоподготовки, Опрос на занятиях, Экзамен
	Итого	3		
9 Состав методов и моделей оценки эффективности КСЗИ.	Проработка лекционного материала	3	ПК-10, ПК-13, ПК-4	Конспект самоподготовки, Опрос на занятиях, Экзамен
	Итого	3		
Итого за семестр		78		
	Подготовка и сдача экзамена	36		Экзамен

8 семестр				
11 Зачёт.	Подготовка к практическим занятиям, семинарам	9	ПК-10, ПК-13, ПК-4	Выступление (доклад) на занятии, Зачет, Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе
	Подготовка к практическим занятиям, семинарам	9		
	Подготовка к практическим занятиям, семинарам	9		
	Подготовка к практическим занятиям, семинарам	9		
	Оформление отчетов по лабораторным работам	30		
	Итого	66		
Итого за семестр		66		
Итого		180		

10. Курсовая работа (проект)

Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсовой работы (проекта) представлены таблице 10.1.

Таблица 10. 1 – Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсовой работы (проекта)

Наименование аудиторных занятий	Трудоемкость,	Формируемые компетенции
8 семестр		
Закрепление знаний по дисциплине «Комплексные системы защиты информации на предприятии», а также получения соответствующих умений и навыков на примере разработки подсистемы технической защиты информации объекта информатизации предприятия.	10	ПК-10, ПК-13, ПК-4
Итого за семестр	10	

10.1 Темы курсовых работ

Примерная тематика курсовых работ (проектов):

- Разработка подсистемы технической защиты выделенного помещения предприятия.
- Разработка подсистемы технической защиты объекта вычислительной техники.
- Разработка подсистемы технической защиты персональных данных, обрабатываемых в информационной системе предприятия.

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
7 семестр				
Выступление (доклад) на	5	10	15	30

занятии				
Конспект самоподготовки	5	5	10	20
Опрос на занятиях	5	5	10	20
Итого максимум за период	15	20	35	70
Экзамен				30
Нарастающим итогом	15	35	70	100
8 семестр				
Выступление (доклад) на занятии	1	2	2	5
Зачет	1	2	2	5
Защита курсовых проектов (работ)	10	15	25	50
Защита отчета	1	2	2	5
Конспект самоподготовки	1	2	2	5
Опрос на занятиях	1	2	2	5
Отчет по курсовой работе	5	5	10	20
Отчет по лабораторной работе	1	2	2	5
Итого максимум за период	21	32	47	100
Нарастающим итогом	21	53	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)

	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, дата обращения: 27.03.2017.

12.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам: Учебное пособие / Голиков А. М. - 2015. 256 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5263, дата обращения: 27.03.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации в инфокоммуникационных системых и сетях: Учебное пособие для практических и семинарских занятий (Часть 1) / Голиков А. М. — 2015. 103 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5330, дата обращения: 27.03.2017.
2. Защита информации в инфокоммуникационных системах и сетях: Сборник лабораторных работ / Голиков А. М. - 2015. 373 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5378, дата обращения: 27.03.2017.
3. Информационные технологии в управлении качеством и защита информации: Методические рекомендации к курсовым работам и организации самостоятельной работы студентов / Годенова Е. Г. — 2011. 35 с. Режим доступа: https://edu.tusur.ru/publications/290, дата обращения: 27.03.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. 1. Базовые законодательные и нормативно-правовые документы РФ в области защиты
2. информации. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 25.03.2017);
3. 2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Лекционные, практические и лабораторные занятия проводятся в специализированных аудиториях кафедры РЗИ. Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебные аудитории, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 407, 412, 416. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 407, 412, 416. Состав оборудования: Учебная мебель; Экран с электроприводом DRAPER BARONET – 1 шт.; Мультимедийный проектор TOSHIBA – 1 шт.; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft SQL-Server 2005; Matlab v6.5

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 4 этаж, ауд. 407,412, 416. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного

аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Комплексные системы защиты информации на предприятии

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **4**
Семестр: **7, 8**

Учебный план набора 2013 года

Разработчики:
- доцент каф. РЗИ А. П. Кшнянкин

Экзамен: 7 семестр
Зачет: 8 семестр
Курсовая работа (проект): 8 семестр

Томск 2017

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Должен знать Основы организации и управления комплексной системой защиты информации на предприятии.; Должен уметь На концептуальном и практическом уровне разрабатывать и внедрять комплексные системы защиты информации на предприятии. ; Должен владеть Навыками внедрения комплексных систем защиты информации на предприятии. ;
ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПК-13

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Основы организации и управления комплексной системой защиты информации на предприятии.	На концептуальном и практическом уровне разрабатывать и внедрять комплексные системы защиты информации на предприятии.	Навыками внедрения комплексных систем защиты информации на предприятии. изменить удалить
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа; • Интерактивные лабораторные занятия; • Лабораторные работы; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа; • Интерактивные лабораторные занятия; • Лабораторные работы; • Контроль самостоятельной работы (курсовой проект / курсовая работа);	• Интерактивные практические занятия; • Самостоятельная работа; • Интерактивные лабораторные занятия; • Лабораторные работы; • Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Отчет по курсовой работе; • Экзамен; • Зачет; • Курсовая работа (проект);	• Конспект самоподготовки; • Опрос на занятиях; • Защита курсовых проектов (работ); • Выступление (доклад) на занятии; • Отчет по курсовой работе; • Экзамен; • Зачет; • Курсовая работа (проект);	• Защита курсовых проектов (работ); • Выступление (доклад) на занятии; • Отчет по курсовой работе; • Экзамен; • Зачет; • Курсовая работа (проект);

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	•Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости.;	•Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.;	•Контролирует работу, проводит оценку, совершенствует действия работы.;
Хорошо (базовый уровень)	•Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.;	•Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования.;	•Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем.;
Удовлетворительно (пороговый уровень)	•Обладает базовыми общими знаниями.;	•Обладает основными умениями, требуемыми для выполнения простых задач;	•Работает при прямом наблюдении.;

2.2 Компетенция ПК-10

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Основы законодательной и нормативно-правовой базы РФ в области информационной безопасности.	Применять требования законодательной и нормативно-правовой базы РФ в области информационной безопасности	Методологией анализа информационной безопасности объектов защиты в соответствие с требованиями законодательной и нормативно-правовой базы РФ в области информационной безопасности.
Виды занятий	•Интерактивные практические занятия; •Интерактивные лекции; •Практические занятия; •Лекции; •Самостоятельная работа; •Интерактивные лабораторные занятия; •Лабораторные работы; •Контроль	•Интерактивные практические занятия; •Интерактивные лекции; •Практические занятия; •Лекции; •Самостоятельная работа; •Интерактивные лабораторные занятия; •Лабораторные работы; •Контроль	•Интерактивные практические занятия; •Самостоятельная работа; •Интерактивные лабораторные занятия; •Лабораторные работы; •Контроль самостоятельной работы (курсовой проект / курсовая работа);

	самостоятельной работы (курсовой проект / курсовая работа);	самостоятельной работы (курсовой проект / курсовая работа);	
Используемые средства оценивания	•Конспект самоподготовки; •Опрос на занятиях; •Выступление (доклад) на занятии; •Отчет по курсовой работе; •Экзамен; •Зачет; •Курсовая работа (проект);	•Конспект самоподготовки; •Опрос на занятиях; •Защита курсовых проектов (работ); •Выступление (доклад) на занятии; •Отчет по курсовой работе; •Экзамен; •Зачет; •Курсовая работа (проект);	•Защита курсовых проектов (работ); •Выступление (доклад) на занятии; •Отчет по курсовой работе; •Экзамен; •Зачет; •Курсовая работа (проект);

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	•Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости.;	•Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.;	•Контролирует работу, проводит оценку, совершенствует действия работы.;
Хорошо (базовый уровень)	•Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.;	•практических умений, требуемых для решения определенных проблем в области исследования.;	•Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем.;
Удовлетворительно (пороговый уровень)	•Обладает базовыми общими знаниями.;	•Обладает основными умениями, требуемыми для выполнения простых задач.;	•Работает при прямом наблюдении.;

2.3 Компетенция ПК-4

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Системные принципы и основы по реализации	Разрабатывать политики информационной	Основами навыков и умений реализовывать

	политики информационной безопасности, применении комплексного подхода к обеспечению информационной безопасности объекта защиты.	безопасности на основе применения комплексного подхода к обеспечению информационной безопасности объекта защиты.	политики информационной безопасности, а также применять комплексный подход к обеспечению информационной безопасности объекта защиты.
Виды занятий	•Интерактивные практические занятия; •Интерактивные лекции; •Практические занятия; •Лекции; •Самостоятельная работа; •Интерактивные лабораторные занятия; •Лабораторные работы; •Контроль самостоятельной работы (курсовой проект / курсовая работа);	•Интерактивные практические занятия; •Интерактивные лекции; •Практические занятия; •Лекции; •Самостоятельная работа; •Интерактивные лабораторные занятия; •Лабораторные работы; •Контроль самостоятельной работы (курсовой проект / курсовая работа);	•Интерактивные практические занятия; •Самостоятельная работа; •Интерактивные лабораторные занятия; •Лабораторные работы; •Контроль самостоятельной работы (курсовой проект / курсовая работа);
Используемые средства оценивания	•Конспект самоподготовки; •Отчет по лабораторной работе; •Опрос на занятиях; •Выступление (доклад) на занятии; •Отчет по курсовой работе; •Экзамен; •Зачет; •Курсовая работа (проект);	•Конспект самоподготовки; •Отчет по лабораторной работе; •Опрос на занятиях; •Защита курсовых проектов (работ); •Выступление (доклад) на занятии; •Отчет по курсовой работе; •Экзамен; •Зачет; •Курсовая работа (проект);	•Отчет по лабораторной работе; •Защита курсовых проектов (работ); •Выступление (доклад) на занятии; •Отчет по курсовой работе; •Экзамен; •Зачет; •Курсовая работа (проект);

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	•Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости.;	•Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.;	•Контролирует работу, проводит оценку, совершенствует действия работы.;

Хорошо (базовый уровень)	•Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.;	•Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования.;	•Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем.;
Удовлетворительно (пороговый уровень)	•Обладает базовыми общими знаниями.;	•Обладает основными умениями, требуемыми для выполнения простых задач.;	•Работает при прямом наблюдении.;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Вопросы на самоподготовку

– 1. Системный подход. Определение и понятие. 2. Система обеспечения информационной безопасности организации. Определение и понятие. 3. Система защиты информации организации. Определение и понятие. 4. Объект защиты информации. Определение и понятие. 5. Защищаемая информация. Определение и понятие. 6. Защита информации. Определение и понятие. 7. Организация защиты информации. Определение и понятие. 8. Техника защиты информации. Определение и понятие. 9. Контроль защиты информации. Цели и понятие. 10. Контролируемая зона. Определение и понятие. 11. Технический канал утечки информации (ТКУИ), виды ТКУИ. Определение, физический смысл. 12.Подсистема технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. Модель и понятие. 13. Подсистема технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. Модель и понятие. 14. Модель угроз подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. 15. Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. 16. Уязвимости системы обеспечения ИБ организации. Определение и понятие. 17. Нарушитель ИБ организации. Определение и понятие. 18. Модель технической реализации ПТЗИ ОИ. 19. Защита информации от несанкционированного доступа (НСД). Определение и понятие. 20. Основа концепции защиты СВТ и АС от НСД к информации. 21. Классификация АС. Цели и основные понятия. 22. Аттестация объектов информатизации. Понятие. 23. Алгоритм приобретения ПЭВМ в защищенном исполнении. 24. Доктрина ИБ РФ. Общие положения.

3.2 Зачёт

– По результатам защиты курсовых проектов

3.3 Темы опросов на занятиях

– Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению комплексной системы защиты информации на предприятии. Специфика курса.

– Цели комплексной защиты информации (ЗИ) и способы ее обеспечения. Системный метод при решении задач обеспечения комплексной защиты информации. Определение возможных каналов утечки информации. Определение объектов и элементов защиты. Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации. Выбор методов и средств защиты информации

– Правовая защита информации. Законодательная база по ЗИ. Сертификация и лицензирование. Правовые нормы, методы и средства защиты охраняемой информации в РФ.

Система юридической ответственности за нарушение норм защиты государственной, служебной и коммерческой тайны в РФ. Правовые основы выявления и предупреждения утечки охраняемой информации. Техническая защита информации. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлектронный). Методы защиты от несанкционированного перехвата речевой, визуальной, оптической, радиоэлектронной информации. Радиомониторинг. Криптографическая защита информации. Средства и методы. Физическая защита информации. Принципы, силы, средства и условия организационной защиты информации. Организация внутриобъектового и пропускного режима предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа). Организация аналитической работы по предупреждению перехвата конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Определение политики защиты информации на предприятии. Особенности организации комплексной защиты информации, отнесенной в установленном порядке к государственной тайне. Определение сил и средств, необходимых для защиты информации.

– Охраняемые сведения и объекты защиты. Особенности отнесения сведений, составляющих служебную, конфиденциальную, коммерческую и государственную тайну к различным степеням и категориям доступа.

– Разработка моделей комплексной системы защиты информации. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ Архитектурное построение комплексной системы защиты информации.

– Структура и содержание технологии управления комплексной системой защиты информации. Планирование и оперативное управление системой ЗИ, управление КСЗИ в условиях чрезвычайных ситуаций. Анализ надежности функционирования комплексной системы защиты информации.

– Организация службы защиты информации (СЗИ) и организационное проектирование деятельности СЗИ. Порядок создания СЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации.

– Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и обеспечение КСЗИ. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИ Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер КСЗИ. Восстановление после чрезвычайной ситуации функций и механизмов КСЗИ организации. Организационная основа процессов восстановления, вопросы системы менеджмента информационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации

– Основные термины и определения, характеризующие эффективность защиты информации. Содержание и особенности методологии оценки эффективности КСЗИ. Основные модели оценки эффективности КСЗИ.

3.4 Темы докладов

– 1. Особенности разработки подсистемы технической защиты объекта вычислительной техники организации. 2. Особенности разработки подсистемы технической защиты защищаемого помещения организации. 3. Особенности разработки подсистемы технической защиты персональных данных, обрабатываемых в информационной системе организации.

3.5 Экзаменационные вопросы

– 1. Системный подход. Определение и понятие. 2. Система обеспечения информационной безопасности организации. Определение и понятие. 3. Система защиты информации организации. Определение и понятие. 4. Объект защиты информации. Определение и понятие. 5. Защищаемая

информация. Определение и понятие. 6. Защита информации. Определение и понятие. 7. Организация защиты информации. Определение и понятие. 8. Техника защиты информации. Определение и понятие. 9. Контроль защиты информации. Цели и понятие. 10. Контролируемая зона. Определение и понятие. 11. Технический канал утечки информации (ТКУИ), виды ТКУИ. Определение, физический смысл. 12.Подсистема технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. Модель и понятие. 13. Подсистема технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. Модель и понятие. 14. Модель угроз подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. 15. Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. 16. Уязвимости системы обеспечения ИБ организации. Определение и понятие. 17. Нарушитель ИБ организации. Определение и понятие. 18. Модель технической реализации ПТЗИ ОИ. 19. Защита информации от несанкционированного доступа (НСД). Определение и понятие. 20. Основа концепции защиты СВТ и АС от НСД к информации. 21. Классификация АС. Цели и основные понятия. 22. Аттестация объектов информатизации. Понятие. 23. Алгоритм приобретения ПЭВМ в защищенном исполнении. 24. Доктрина ИБ РФ. Общие положения.

3.6 Темы лабораторных работ

- Система защиты информации от несанкционированного доступа SecretNet.
- Система защиты информации от несанкционированного доступа Dallas Lock.
- Система защиты информации от несанкционированного доступа Страж NT.
- DLP-решения по защите информации в информационных системах.
- Защита информации от программных воздействий на базе антивируса Dr.Web.
- Защита информации от программных воздействий на базе антивируса KAV.

3.7 Темы курсовых проектов (работ)

- 1 Разработка подсистемы технической защиты выделенного помещения предприятия. 2. Разработка подсистемы технической защиты объекта вычислительной техники. 3.Разработка подсистемы технической защиты персональных данных, обрабатываемых в информационной системе предприятия.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

2. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, дата обращения: 27.03.2017.

4.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам: Учебное пособие / Голиков А. М. - 2015. 256 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5263, дата обращения: 27.03.2017.

4.3. Обязательные учебно-методические пособия

1. Защита информации в инфокоммуникационных системых и сетях: Учебное пособие для практических и семинарских занятий (Часть 1) / Голиков А. М. — 2015. 103 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5330, дата обращения: 27.03.2017.
2. Защита информации в инфокоммуникационных системах и сетях: Сборник лабораторных работ / Голиков А. М. - 2015. 373 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5378, дата обращения: 27.03.2017.

3. Информационные технологии в управлении качеством и защита информации: Методические рекомендации к курсовым работам и организации самостоятельной работы студентов / Годенова Е. Г. — 2011. 35 с. Режим доступа: https://edu.tusur.ru/publications/290, дата обращения: 27.03.2017.

4.4. Базы данных, информационно справочные и поисковые системы

1. 1. Базовые законодательные и нормативно-правовые документы РФ в области защиты
2. информации. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 25.03.2017);
3. 2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru